Limits and enablers of data sharing

Graef, Inge; Tombal, Thomas; De Streel, Alexandre

Published in:
TILEC discussion papers

Publication date:
2019

Document Version
Publisher's PDF, also known as Version of record

TILBURG UNIVERSITY

TILEC

TILEC Discussion Paper

DP 2019-024

Limits and Enablers of Data Sharing
An Analytical Framework for EU Competition, Data Protection and Consumer Law

By

Inge Graef, Thomas Tombal and Alexandre Streel

November 2019

ISSN 1572-4042

ISSN 2213-9419 http://ssrn.com/abstract=3494212

Limits and Enablers of Data Sharing
An Analytical Framework for EU Competition, Data Protection and Consumer Law[1]

Inge Graef,[2] Thomas Tombal[3] & Alexandre de Streel[4]

Abstract:
Data sharing presents many opportunities in terms of stimulating innovation and creating a level playing field between businesses, but also carries risks by potentially decreasing incentives for data collection and analysis, facilitating collusion between firms or exploiting consumers as well as undermining privacy. The paper maps the limits and enablers of data sharing in the fields of EU competition, data protection and consumer law and illustrates how an optimal regulatory framework for data sharing can maximise the benefits while minimising the risks. The paper sets out an analytical framework for data sharing by outlining how the three regimes complement each other in either limiting or enabling data sharing, and by outlining the tensions within and between these three regimes. Considering their different scope, it is of the utmost importance that the three legal instruments are applied consistently. This means, on the one hand, that any conflict should be alleviated or minimised and, on the other hand, that the instruments should be applied more as complements than as substitutes. Such an objective can only be achieved if the authorities in charge of enforcement of the different legal instruments cooperate closely with each other to ensure consistent and complementary interpretation. The paper concludes that the three horizontal instruments, if implemented effectively, already facilitate or even impose the sharing of data in many circumstances. As a result, the existing horizontal rules should be complemented with new sectoral rules only when they have proved to be insufficient given the particular characteristics of the sector.

Key words: data portability, data access, innovation, competition, data protection, consumer protection, collusion, privacy

JEL codes: K20, K21, K30, L43, O38

[1] This paper was prepared in the context of the Digital Clearinghouse project, which brings together competition, data protection and consumer authorities to exchange insights about how to better protect individuals in digital markets. The project is organised by the University of Namur, the University of Tilburg and the European Policy Centre with funding of the Open Society Foundations, Omidyar Network and the King Baudouin Foundation. Please visit the website: https://www.digitalclearinghouse.org/
[2] Assistant Professor at Tilburg University, affiliated to the Tilburg Law & Economics Center (TILEC) and the Tilburg Institute for Law, Technology, and Society (TILT).
[3] PhD researcher at the University of Namur, affiliated to CRIDS/NADI.
[4] Professor at the University of Namur, affiliated to CRIDS/NADI and CERRE.

Table of Contents

1. Introduction

1.1. Scope of the paper

Data is regarded as an essential resource for innovation, economic growth, and societal progress in various fields, ranging from health, agriculture and energy to intelligent transport systems, finance and smart cities.[5] To unleash the full potential of data for the economy, mechanisms to create wider accessibility and reuse of data across private and public actors are now being devised in many areas of our lives. Although data sharing is generally seen as beneficial for welfare,[6] the exchange of data can also lead to concerns regarding privacy, collusion or consumer protection when it enables market players to exploit consumers.

This paper maps how competition, data protection and consumer law position themselves towards data sharing. A neutral stance is taken, implying that we do not aim to argue in favour or against data sharing. Instead, the objective of the paper is to analyse to what extent competition, data protection and consumer law either limit or enable data sharing. Because the focus is purely on a legal analysis, economic, ethical, technical and other insights about the feasibility and desirability of data sharing are not considered. Our findings can inform debates about the design of new data sharing regimes by pointing out the limits and enablers of data sharing under the three horizontal regimes that are applicable to all sectors of the economy.

For a number of industries, sector-specific regimes relating to data sharing already exist, including the Payment Services Directive 2 (access-to-account rule)[7] and the new Electricity Directive (access to metering and consumption data).[8] In addition, a code of conduct on data sharing has been adopted by market players in the agricultural sector[9] and discussions about data sharing in the automotive sector[10] are ongoing. The paper does not analyse these sector-specific regimes. Instead, it aims to draw lessons from how the regimes of competition, data protection and consumer law interact in stimulating and restricting data sharing. Lessons drawn are relevant for these sectors too, as the existence of sector-specific legislation does not preclude the applicability of horizontal regimes such as competition, data protection and consumer law. We use the notion 'data sharing' as an umbrella term referring to the various ways in which data can be exchanged. This includes access to (ability to look at and potentially use the data, depending on the conditions set by the regime at stake) as well as portability of data (ability to transfer or copy data). The paper does not analyse Government-to-Business data sharing as covered by the Open Data and Public Sector Information Directive[11], nor is Business-to-Government data sharing covered.[12] Relevant dimensions of data sharing for our purposes are: Business-to-Business, Business-to-Consumer as well as Business-to-Consumer-to-business (where for instance a consumer requests access to or portability of data that is then shared with another provider).

At the outset, it is worthwhile to keep in mind the objectives of the three regimes under investigation. All three regimes contribute to the integration of the internal market and protect the welfare of consumers or

[5] Communication from the Commission, 'Building a European Data Economy, COM (2017) 9, p. 2 and 8.
[6] Mayer-Schonberger and Ramge (2018).
[7] Articles 66 and 67 of Directive 2015/2366 of 25 November 2015 on payment services in the internal market [2015] OJ L 337/35.
[8] Article 23(1) of Directive 2019/944 of the European Parliament and of the Council of 5 June 2019 on common rules for the internal market for electricity [2019] OJ L 158/125.
[9] EU Code of conduct on agricultural data sharing by contractual agreement, April 2018, available at https://copa-cogeca.eu/img/user/files/EU%20CODE/EU_Code_2018_web_version.pdf.
[10] Commission, 'On the road to automated mobility: An EU strategy for mobility of the future' (Communication) COM (2018) 283 final, p. 13.
[11] Directive 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information [2019] OJ L 172/56.
[12] Business-to-Government data sharing is discussed in Commission Staff Working Document 'Guidance on sharing private sector data, SWD (2018) 125.

data subjects. Although there is an overlap in objectives, the means by which the objectives are pursued differ. Competition law tries to protect consumer welfare by intervening against anticompetitive behaviour, consumer law aims to assist consumers as the weaker party in market transactions and data protection law provides data subjects with control over their personal data and partly has a basis in fundamental rights protection.[13] Because of their different scope of protection, the three regimes can complement each other but may also conflict in how they treat data sharing.

Table 1: Comparison between the goals and scope of the legal instruments

Types of legal instrument	**Competition protection**	**Consumer protection**	**Personal data protection**
Main Objectives	Economic total or consumer welfare and beyond	Transparency and fairness in possibly unbalanced transactions	Data subject privacy and self-determination
Scope	Transactions made by undertakings	Mainly B2C transactions	Transactions relying on personal data

In light of the above, the goal of this paper is two-fold. First, it presents the dual relationship that competition, personal data protection and consumer law have with data sharing. Indeed, while these three fields of law can potentially limit data sharing (Section 2), they can also enable it (Section 3). Second, it will draw an analytical framework for data sharing by outlining how these regimes complement each other, on the one hand, and by outlining the tensions within and between these three regimes, on the other hand (Section 4).

1.2. Definition and characteristics of data

Personal and non-personal data play an increasing role in the economy and society as they can be collected cheaply with the deployment of connected devices and they can be analysed more usefully with the development of Artificial Intelligence techniques. Digital data can be defined as 'machine-readable encoded information'[14] while big data can be defined as 'the information asset characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value'[15].[16]

Thus, the value and interest of data is in the information and the knowledge that may be inferred from such data.[17] Information sciences use the concept of a data pyramid to explain the relationship between data, information and knowledge[18] and such a pyramid may be applied to the data value chain as explained by Gal and Rubinfeld (2019). This value chain comprises several links: (i) first, raw personal and non-personal data are collected directly or bought on a secondary data market; (ii) second, data are structured and turned into information; (iii) third, those structured data are analysed by algorithms and information is turned into knowledge, such as a prediction; and finally (iv) the analysis of the structured data leads to an action such

[13] See Graef (2018a:121-151).
[14] Zech (2016).
[15] De Mauro et al. (2016).
[16] For definition and categories of data, see also Autorité de la concurrence and Bundeskartellamt (2016:4-7).
[17] Interestingly, EU law generally refers to information or knowledge. Article 4(1) GDPR 2016/679 refers to personal data defined as 'any *information* relating to an identified or identifiable natural person'; Article 2(3a) of the Public Sector Information Directive 2003/98 refers to *document* defined as any content whatever its medium (written on paper or stored in electronic form or as a sound, visual or audio-visual recording); Article 3(1) of the Free-flow of non-personal data Regulation 2018/1807 refers to data defined as data other than personal data as defined in the GDPR.
[18] As explained by Varian (2019).

as improving products or offerings.[19] Going down the value chain, the efforts and investments by the data owner increase and may even be protected by intellectual property rights. Hence, the interest in protecting property and investment incentives, which is one part of the balance when deciding to impose access, increases.

Figure 1: Data pyramid and the big data value chain

Data pyramid	Big data value chain
Data	Collection
Information	Structure
Knowledge	Analysis
Action	Use

Source: Adapted from Gal and Rubinfeld (2019) and Varian (2019)

In practice, a request for data access may take place at different levels of the value chain. An access seeker may request access to raw data and then carry out other downstream operations, *i.e.* structure, analyse and use the data. An access seeker may also request access to the structure and then possibly collect and analyse the data. The access seeker may also ask access to the full suite (*i.e.* the data collected, structured and analysed) to take their own course of action.

- Characteristics of data and competitive dynamics of the data economy

Data and big data have been characterised in many ways[20] but the one proposed by the OECD (2015:179) is one of the best: data constitute an infrastructure or *infrastructural resources* that meet the following criteria.

- Data are a non-rivalrous good as they can be shared without losing their value, hence data access is often equated to data sharing;
- Data are a capital good as they are often used as an input in developing other products. This is particularly the case for machine learning where data are the raw material for the algorithm;
- Data are a general-purpose input[21] that can be used and re-used to develop different products, for instance the same behavioural data can be used to develop a fraud detection algorithm or a tastes prediction algorithm.[22]

The collection, structuring or the analysis of data may be subject to legal, technological and economic entry barriers. For data collection, legal barriers may be found in legislation (in particular privacy laws that strictly regulate the collection of personal data) or in contracts that may contain exclusivity clauses prohibiting data transfer.[23] Barriers may also be technical, for instance when data are encrypted. Finally, barriers may be economic when collecting data present economies of scale and scope or network effects. This is often the case in practice as many data are collected, in multi-sided market settings, against 'free' services that exhibit important network effects.[24] For instance, it is easier and less costly for a large social network such as

[19] Gal and Rubinfeld (2019) mentioned an additional link of data storage which is not mentioned here. See also de Streel (2018).
[20] Cyril Ritter presented a long list of different data characterisations: beautiful, everywhere, the new oil, truth, the new currency, the new gold, the new electricity, the new air, the new coal, the new champagne, like water, like sunshine, like silk, like a bikini, like teenage sex, like astrology, like garbage, like waste, like toxic waste, like nuclear waste.
[21] Bresnahan and Trajtenberg (1995) give the three main characteristics of general-purpose technologies: pervasiveness, the inherent potential for technical improvements and the innovational complementarities of the former
[22] This is in particular the case in the digital sector where innovation is often based on different modules that are multi-purposes: Bourreau and de Streel (2019).
[23] See Osborne Clark (2016).
[24] Next to the network effects for data collection alone, there are some monetisation and customer feedback loops between data collection and data analysis which may increase even further the entry barriers in data collection: see Lerner (2014). As always, the effects of those feedback loops is an empirical issue that should be analysed on a case-by-case: de Streel (2018).

Facebook to collect users' data because they can attract users more easily given the direct network effects. Similarly, it is less costly for a large search engine such as Google to attract more search queries because they can attract users more easily given the indirect network effects.[25]

With regard to data structuring, legal barriers may be found in legislation protecting property(-like) rights (such as database or trade secrets)[26] or in contracts. Barriers may also be technical, for instance when structured data are not interoperable.[27] Finally, barriers may be economic because the data structures often exhibit important network effects as 'they allow data to be communicated between different market players active at different level of the value chain'.[28] For instance, the 1860 brick structure of IMS-Health had become a *de facto* industry standard.

Regarding data analysis, barriers may be legal, in particular privacy laws that limit data processing. Barriers are often economic because big data analysis exhibits important economies of scale and scope. The level of economies of scale (the volume of the data) is not easy to determine and depends very much on the type of data and the type of analysis as shown by Junqué de Fortuny et al. (2013). For instance, for search algorithm. Microsoft argued, in *Microsoft/Yahoo! Search Business*, that with larger scale a search engine can run tests on how to improve the algorithm and that it is possible to experiment more and faster as traffic volume increases because experimental traffic will take up a smaller proportion of overall traffic.[29] Economies of scope (the variety of data) may be even more important than economies of scale but they are equally difficult to assess.[30] Already in *Google/DoubleClick*, the Commission observed that: 'competition based on the quality of collected data thus is not only decided by virtue of the sheer size of the respective databases, but also determined by the different types of data the competitors have access to and the question which type eventually will prove to be the most useful for internet advertising purposes.'[31]

2. Limits to data sharing

Competition, personal data protection and consumer law can, to some extent, limit data sharing. Indeed, competition law might intervene to sanction data pooling initiatives, or to prevent the combination of datasets through merger, entailing competition concerns. Moreover, the principles of purpose limitation and data minimisation contained in the General Data Protection Regulation[32] (hereafter "GDPR") might also limit data sharing. Additionally, consumer law can also restrict data sharing.

2.1. Data pooling and collusion concerns

[25] Prufer and Schottmuller (2017).

[26] Directive 96/9 of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases, OJ [1996] L 77/20; Directive 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, OJ [2016] L 157/1. See Drexl (2016:19-30).

[27] Deloitte et al. (2018). Kerber and Schweitzer (2017:40) define interoperability as: 'the ability of a system, product or service to communicate and function with other (technically different) systems, products or services'. Varian (2019) observes that: 'Constructing this data pipeline is often the most labor intensive and expensive part of building a data infrastructure, since different businesses often have idiosyncratic legacy systems that are difficult to interconnect'.

[28] Drexl (2016:54).

[29] Commission Decision of 18 February 2010, Case M. 5727 *Microsoft/Yahoo! Search Business*, par. 162 and 223. Lerner (2014:37), Lambrecht and Trucker (2015:10) or Sokol and Comerford (2016) submit that the scale economies are low even for tail queries and that there is a diminishing marginal return of data both for head and tail queries while Mc Afee (2015) cautious that more data matters for tail queries.

[30] The UK Information Commissioner's Office (2014, para 25) observes that variety is the most important characteristic of big data.

[31] Commission Decision of 11 March 2008, Case M.4731 *Google/ DoubleClick*, para. 273.

[32] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *OJ L 119*, 4 May 2016.

Sharing of commercially sensitive information among competitors can violate Article 101 TFEU, which prohibits restrictive agreements and concerted practices. How Article 101 TFEU is to be applied to data pooling arrangements, whereby firms agree to share information among each other relating to a particular market, service or industry,[33] is not yet clear. Article 101 TFEU can stand in the way of data sharing in situations where the exchange of information among competitors gives rise to collusion under Article 101(1) TFEU and the resulting restriction of competition cannot be justified under Article 101(3) TFEU by showing that the procompetitive effects outweigh the anticompetitive effects.

In *Asnef-Equifax*, the Court of Justice was asked to assess the compatibility with Article 101 TFEU of a register set up by financial institutions in Spain involving the exchange of solvency and credit information about their customers in order to evaluate the risks of engaging in lending and credit activities. The Court argued that in order not to restrict competition under Article 101 TFEU: (1) the relevant market at stake should not be highly concentrated; (2) the register should not be capable of revealing the identity of the lenders, as this could help to identify the market position or commercial strategy of competitors; and (3) the register should be accessible in a non-discriminatory manner to all operators active in the relevant sphere, so that some operators are not put at a disadvantage if they do not have access to information needed for risk assessment.[34] These three conditions could also be applied to assess data pooling arrangements where information about individual customers is shared among market players.

The Commission *Horizontal Agreements Guidelines* pay attention to how certain factors can make the exchange of information among competitors more problematic, including the strategic nature of the information, the market coverage of the firms involved, the individualised or aggregated nature of the company information exchanged, the age of the data, the frequency of the information exchange, the public or non-public nature of the information, and whether the exchange of information is public or non-public.[35]

Most illustrative is the investigation the Commission opened in May 2019 into the data pooling system of *Insurance Ireland*, which is an association bringing together companies active in the insurance sector in Ireland. As part of its activities, Insurance Ireland administers a database to which member companies contribute insurance claims data on an ongoing basis. According to the Commission's press release, the objective of the system is "*to facilitate the detection of potentially fraudulent behaviour by insurance claimants and to ensure the accuracy of information provided by potential customers to insurance companies and/or their agents*".[36] While the Commission acknowledges that such a data pooling system may benefit consumers by ensuring more suitable products and competitive prices, it is concerned in particular about whether the conditions of access to the system of Insurance Ireland restrict competition and thereby reduce Irish drivers' choice of insurance policies.[37]

Apart from listing the factual circumstances of the case, the press release also provides a more general background as to the Commission's current thinking about data pooling. The Commission states that data pooling arrangements are often pro-competitive: (1) they directly benefit consumers by enabling effective competition on the market, as service providers may be able to offer better prices and services to consumers by accessing and participating in a data pool; and (2) access to data in a data pool may enable effective market entry, resulting into improved choice of services and suppliers to the benefit of consumers.

[33] This is the definition used by Lundqvist, see B. Lundqvist, 'Competition and Data Pools', Journal of European Consumer and Market Law 2018, p. 146.
[34] Case C-238/05 *Asnef-Equifax*, EU:C:2006:734, par. 58-61.
[35] Commission Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements [2011] OJ C 11/1, par. 86-94.
[36] Press release European Commission, 'Antitrust: Commission opens investigation into Insurance Ireland data pooling system', 14 May 2019, available at https://europa.eu/rapid/press-release_IP-19-2509_en.htm.
[37] *Ibidem*.

However, the Commission also points out that data pooling arrangements may in some situations lead to restrictions of competition, for instance when: (1) the conditions of access to and participation in a data pool result in placing certain market players at a competitive disadvantage; or (2) the data pooling system enables market players to become aware of the market strategies of their competitors.[38] The Commission intends to launch a review of its Guidelines on horizontal cooperation agreements (Horizontal Guidelines), which provide the general principles on how to assess information exchanges among competitors. This review takes place against the background of the upcoming expiry of the Research & Development Block Exemption Regulation and the Specialisation Block Exemption Regulation.[39]

Beyond restrictions on access to the pool on which the investigation of the Commission against Insurance Ireland focuses, another question is when the existence of data pooling arrangements in themselves can breach Article 101 TFEU through the exchange of commercially sensitive information among competitors. In this regard, Lundqvist makes a distinction between three situations. Whereas exchange of technical information for the development of new products or interoperability among existing products through a data pool seems largely unproblematic, data pooling arrangements where parties share strategic and competitive information regarding prices or new innovations have to be considered as potentially breaching Article 101 TFEU. Within those two extremes lie data pools in which not directly commercially sensitive information is shared but where information is exchanged about a large number of customers in a way that may ultimately enable a member to the pool to extract competitive insights based on data analytics.[40]
In its upcoming revision of the Horizontal Guidelines, the Commission will likely and hopefully clarify how these existing indicators have to be applied to assess the more complicated data pooling arrangements where possible anticompetitive effects are less pronounced than in previous cases. Finally, the exchange of data among competitors can also take another shape.

Reference can be made in this regard to the investigation that the Commission opened against *Amazon* in July 2019. According to the press release, the Commission will assess whether Amazon's use of sensitive information from independent retailers violates Article 101 and 102 TFEU considering its dual role as a retailer and provider of a marketplace where it competes with the independent retailers.[41] Although Amazon does not negotiate these agreements but imposes them as standard contracts on independent retailers, the investigation can shed further light on the boundaries of competition liability for the exchange of commercially sensitive information among competitors.

2.2. Combination of datasets in mergers and competition concerns[42]

The EU Merger Regulation can stand in the way of data sharing between merging parties when the combination of previously separate datasets would "*significantly impede effective competition* […] *in particular as a result of the creation or strengthening of a dominant position*".[43] The European Commission has analysed competition concerns relating to the combination of data a number of times in merger decisions. So far, the Commission has not yet blocked a merger on the ground that the combination of data would give rise to competition concerns. Nevertheless, Competition Commissioner Vestager does refer to the possibility that data concentration can constitute a basis for a competition case in her public statements. For instance, in a February 2019 speech she stated: "[c]*ompetition can't work if just a few companies control a vital resource that you need to be able to compete – and if they refuse to share it with others. Right now,*

[38] *Ibidem*
[39] *Ibidem*
[40] Lundqvist (2018:150).
[41] Press release European Commission, 'Antitrust: Commission opens investigation into possible anti-competitive conduct of Amazon', 17 July 2019, available at https://europa.eu/rapid/press-release_IP-19-4291_en.htm.
[42] This section is partly based on Graef (2018b).
[43] Article 2(3) of Council Regulation 139/2004 of 20 January 2004 on the control of concentrations between undertakings (Merger Regulation) [2004] OJ L 24/1.

it looks as though data is becoming one of those vital resources. And if that's so in a particular case, then we need to make sure it's not monopolised by a few".[44]

In its 2007 *Google/DoubleClick* merger decision, the Commission argued that the combination of Google's data on users' search behaviour with DoubleClick's data on web-browsing behaviour of users would not give the merged entity a competitive advantage that could not be matched by competitors.[45] According to the Commission, such a combination of information was already available to a number of Google's competitors, including Microsoft and Yahoo which both ran search engines and offered ad serving at that time as well. In addition, the Commission argued that competitors could purchase data or targeting services from third parties including portals, other major web publishers and internet service providers.[46]

In 2014, the Commission analysed data-related competition concerns in *Facebook/WhatsApp*. According to the Commission, the acquisition of WhatsApp would not increase the amount of data potentially available to Facebook for advertising purposes because WhatsApp did not collect data valuable for advertising purposes at the time of the merger.[47] The Commission still investigated possible theories of harm relating to data concentration to the extent that it was likely to strengthen Facebook's position in the market for online advertising. In this regard, the Commission argued that the merger would not raise competition concerns even if Facebook would introduce targeted advertising on WhatsApp or start collecting data from WhatsApp users with a view to improving the accuracy of the targeted ads served on Facebook's social networking platform.[48] In the Commission's view, there would continue to be a sufficient number of alternative providers to Facebook for the supply of targeted advertising after the merger, and a large amount of internet user data that are valuable for advertising purposes were not within Facebook's exclusive control. In particular, the Commission considered Google, Apple, Amazon, eBay, Microsoft, AOL, Yahoo!, Twitter, IAC, LinkedIn, Adobe and Yelp as market participants that collect user data alongside Facebook.[49] Whereas the Commission in *Facebook/WhatsApp* had not defined a possible market for data or data analytics services on the ground that "*neither of the Parties is currently active in any such potential markets*",[50] an evolution is visible in *Microsoft/LinkedIn*. Under the assumption that such data combination is allowed under the applicable data protection legislation, the Commission distinguished two main ways in which the *Microsoft/LinkedIn* merger could raise competition concerns as a result of the combination of data. First, the Commission acknowledged that the combination of two datasets as a result of a merger may "*increase the merged entity's market power in a hypothetical market for the supply of this data or increase barriers to entry/expansion in the market for actual or potential competitors, which may need this data to operate on this market*". Second, the Commission made clear that, even if there is no intention or technical possibility to combine the two datasets, "*it may be that pre-merger the two companies were competing with*

[44] Speech Competition Commissioner Vestager, 'Making the data revolution work for us', Mackenzie Stuart Lecture, Cambridge, 4 February 2019, available at https://ec.europa.eu/commission/commissioners/2014-2019/vestager/announcements/making-data-revolution-work-us_en.
[45] Case COMP/M.4731 – *Google/ DoubleClick*, 11 March 2008, par. 366.
[46] Case COMP/M.4731 – *Google/ DoubleClick*, 11 March 2008, par. 269-272 and 365.
[47] Case COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, par. 166.
[48] In May 2017, the Commission imposed a 110 million euro fine on Facebook for providing misleading information during the merger investigation. While Facebook had informed the Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' accounts, WhatsApp announced updates to its terms of service in August 2016 including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. However, the fact that misleading information was given did not impact the 2014 authorisation of the transaction as the decision was based on a number of elements going beyond automated user matching and the Commission at the time carried out an 'even if' assessment assuming user matching as a possibility (Press release European Commission, 'Mergers: Commission fines Facebook €110 million for providing misleading information about WhatsApp takeover', 18 May 2017, available at http://europa.eu/rapid/press-release_IP-17-1369_en.htm).
[49] Case COMP/M.7217 – *Facebook/WhatsApp*, 3 October 2014, par. 187-190.
[50] *Ibidem*, par. 72.

each other on the basis of the data they controlled and this competition would be eliminated by the merger".[51]

These two ways distinguished in *Microsoft/LinkedIn* as to how a combination of data may raise competition concerns in a merger have also been referred to by the Commission as the relevant legal framework in its *Verizon/Yahoo* merger decision.[52] Despite this evolution in approach, the Commission nevertheless came to the same conclusion in *Microsoft/LinkedIn* as in *Google/DoubleClick* and *Facebook/WhatsApp*, namely that the combination of data enabled did not raise serious doubts as to the merger's compatibility with the internal market in relation to online advertising.[53] The Commission specified three grounds for this. First, Microsoft and LinkedIn did not make available their data to third parties for advertising purposes, with only very limited exceptions. Second, the combination of their respective datasets did not appear to result in raising the barriers to entry/expansion for other players in this space, as there would continue to be a large amount of internet user data that were valuable for advertising purposes and that were not within Microsoft's exclusive control. Third, the merging parties were small market players and competed with each other only to a very limited extent in online advertising and its possible segments.[54]

In its 2018 *Apple/Shazam* merger decision, the Commission again reached the conclusion that the combination of the datasets of the two companies would not give rise to competition concerns. This time the focus was not on online advertising but on digital music streaming apps where Apple is active with its Apple Music service and Shazam offers a leading music recognition application. According to the Commission, it would be unlikely that the merged entity would have the ability to foreclose competing providers of digital music streaming apps even if Shazam's data would be integrated into Apple's dataset. Shazam's data, in the Commission's view, does not seem to be an important input to improve existing functionalities or offer additional functionalities within digital music streaming apps, and does not appear to be unique based on a comparison with other alternative datasets in relation to the metrics associated with the Four V's of big data, namely the variety of data, the speed at which the data is collected (velocity), the size of the dataset (volume), and its economic relevance (value).[55]

The analysis of these data-related merger decisions shows that the Commission does not shy away from analysing the impact of the combination of data through a merger. Nevertheless, one can raise the question whether the reasoning of the Commission in these cases has always been credible considering the – often – general reference to the alleged wide availability of remaining data held by third parties without analysing the substitutability of the particular type of data affected in more detail. Even though we have not seen such cases yet, the Commission may decide to block the merger altogether or to impose remedies if a concentration of data in the hands of one entity would significantly impede effective competition in the relevant market. To address these competition concerns, the Commission could mandate the establishment of a firewall between the different datasets.[56] Such a remedy would limit data sharing in an effort to protect against anticompetitive effects. As will be discussed in section 3, a remedy to address data-related competition concerns in a merger can interestingly also be designed as an enabler of data sharing when it involves a divestiture of data to a third party.

---

[51] Case M.8124 – *Microsoft/LinkedIn*, 6 December 2016, par. 179.
[52] Case M.8180 – *Verizon/Yahoo*, 21 December 2016, par. 81-83.
[53] The Commission reached the same conclusion in *Verizon/Yahoo*, see Case M.8180 – *Verizon/Yahoo*, 21 December 2016, par. 89-93.
[54] Case M.8124 – *Microsoft / LinkedIn*, 6 December 2016, par. 180. The Commission similarly investigated a hypothetical market for data in two other instances in the Microsoft/LinkedIn decision, namely in the context of customer relationship management software solutions and with regard to the use of data for machine learning in productivity software solutions. For both instances, the Commission concluded that the transaction did not raise serious doubts as to its compatibility with the internal market. See Case M.8124 – *Microsoft / LinkedIn*, 6 December 2016, par. 253-264 and 373-381. For an analysis, see Graef (2018b: 79-81).
[55] Case M.8788 – *Apple/Shazam*, 6 September 2018, par. 313-330.
[56] This is the remedy former FTC Commissioner Pamela Jones Harbour suggested in the US *Google/DoubleClick* merger. See her dissenting Statement in *Google/DoubleClick*, FTC File No. 071-0170, 20 December 2007, footnote 23 on page 9.

2.3. Purpose limitation and data minimisation principles in the GDPR

The processing[57] of personal data, defined as "*any information relating to an identified or identifiable natural person*"[58], is regulated by the GDPR. As data sharing might entail the exchange of personal data, which is considered as an act of processing falling under the scope of the GDPR, this Regulation has to be taken into account. While the GDPR does not forbid, as such, the sharing of personal data, it nevertheless limits the possibilities of data sharing. This is because this instrument aims at reaching an equilibrium between the fundamental right of the protection of personal data, on the one hand, and the fundamental right of the freedom to conduct a business, on the other hand.[59] To do so, the GDPR gives to the data subjects[60] a form of control over "their" personal data, and subjects the processing of personal data by controllers[61] to several principles contained in Article 5 of the GDPR. Two of these principles potentially limit data sharing, namely the principles of purpose limitation and data minimisation.[62]

According to the *purpose limitation principle*, personal data can only be processed for specified, explicit and legitimate purposes, and cannot be further processed in a manner that is incompatible with those purposes.[63] This means that data that has been collected for a specific purpose cannot be shared with third parties if this act of sharing does not fit within this initial purpose. Because the act of sharing is a new processing activity, distinct from the initial one, it requires a lawful basis.[64] However, according to Article 6.4 of the GDPR, a separate lawful basis is only necessary if the new purpose (*in casu* the data sharing) is not compatible with the initial purpose for which the data has been collected. Conversely, according to Recital 50 of the GDPR, if this new purpose is compatible with the initial purpose, no separate lawful basis is required. To assess this compatibility, a key consideration will be whether the data subjects could have reasonably expected that the data holder would have shared this data. Yet, the affirmation that a separate lawful basis is not necessary if the further processing is compatible with the initial processing is controversial.[65]

According to the *data minimisation principle*, only the adequate, relevant and necessary personal data for the fulfilment of a specific purpose can be processed.[66] This implies that, even if the act of data sharing complies with the purpose limitation principle, the categories and amount of data that can be shared should nevertheless be limited to what is necessary to meet this purpose. This outlines the importance of clearly

[57] "*Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4.2 of the GDPR).
[58] Article 4.1 of the GDPR. An identifiable natural person is "*one who can be identified, directly or indirectly, in particular by reference to an identifier*". This definition is further refined by Recital 26 of the GDPR: "*To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments*".
[59] Recital 4 of the GDPR. Resp. Articles 8 and 16 of the Charter of Fundamental Rights of the European Union.
[60] "*Any identified or identifiable natural person*" (Article 4.1 of the GDPR).
[61] "*The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data*" (Art. 4.7 of the GDPR).
[62] Article 5.1.b) and c) of the GDPR.
[63] Article 5.1.b) of the GDPR.
[64] These lawful bases are listed in Article 6 of the GDPR.
[65] Wendehorst (2017: 335-336).
[66] Article 5.1.c) of the GDPR.

defining the specific purpose of the data sharing, as the GDPR prevents "over-sharing", i.e. sharing more data than what is relevant and necessary for the purpose of the processing.

Outlining how these two principles of the GDPR might limit the sharing of personal data is important. Indeed, the notion of personal data is dynamic and ever-expanding[67] and this creates uncertainties about the scope of the GDPR. Yet, the dichotomy between personal and non-personal data is broadly relied upon in the legal framework[68]. This can however be rather artificial in some cases, as it might not be easy to determine whether specific data should be considered as personal or not. This is even more so if one considers the constant development of *Big Data*[69] analytics. Indeed, *Big Data* increases the possibility of "crossing" multiple data sets, to which it was previously more difficult to have access. This consequently exacerbates the risk of direct or indirect re-identification of a data subject on the basis of these data, whether by the controller or by a third party. In doing so, data considered at a time "T" as non-personal may thus, on the basis of technological developments in data analytics capabilities, become personal data at time "T+1". Therefore, as more and more data might be considered as being personal, the limitations on data sharing imposed by the purpose limitation and data minimisation principles of the GDPR could have a strong impact in practice.

2.4. Consumer law

The consumer law regime can impose obligations on traders restricting their ability to use or share data. According to the Unfair Contract Terms Directive, a non-individually negotiated contractual term is to be regarded as unfair if "*contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer*".[70] This could include terms that force consumers to share their data with a third party as illustrated by the actions taken against WhatsApp in Italy in May 2017. The Italian competition and consumer authority took two decisions imposing a fine of 3 million euro on WhatsApp for alleged unfair commercial practices and inclusion of unfair terms, including the provision forcing users to share their personal data with Facebook by making them believe that otherwise they would not have been able to continue using the service.[71]

In November 2018, the Italian competition and consumer authority also imposed a fine on Facebook for misleading consumers into registering an account without adequately informing them of the commercial use of their data and for exerting undue influence on registered users who suffered from unconscious and automatic transmission of their data from Facebook to third parties for commercial purposes. The Italian authority qualified the latter conduct as an aggressive commercial practice. Even though consumers could limit their consent, they were then faced with significant restrictions on their use of Facebook's social network and third-party websites which induced them to maintain the pre-selection by Facebook of the broadest consent to data sharing.[72]

---

[67] Article 4.1 of the GDPR.
[68] For a criticism of this broad reliance on the personal versus non-personal data dichotomy, see: Graef, Gellert and Husovec, (2019: 605-621).
[69] "*"Big data" is a field that treats ways to analyze, systematically extract information from, or otherwise deal with data sets that are too large or complex to be dealt with by traditional data-processing application software*" (https://en.wikipedia.org/wiki/Big_data).
[70] Article 3(1) of Council Directive 93/13 of 5 April 1993 on unfair terms in consumer contracts [1993] OJ L 95/29.
[71] Press release Autorità garante della concorrenza e del mercato, 'WhatsApp fined for 3 million euro for having forced its users to share their personal data with Facebook', 12 May 2017, available at https://en.agcm.it/en/media/press-releases/2017/5/alias-2380. For an analysis, see Zingales (2017: 557-558).
[72] Press release Autorità garante della concorrenza e del mercato, 'Facebook fined 10 million Euros by the ICA for unfair commercial practices for using its subscribers' data for commercial purposes', 7 December 2018, available at https://en.agcm.it/en/media/press-releases/2018/12/Facebook-fined-10-million-Euros-by-the-ICA-for-unfair-commercial-practices-for-using-its-subscribers%E2%80%99-data-for-commercial-purposes

Another example of the relevance of consumer law is how Facebook updated its terms in April 2019 to clarify how it relies on users' data to develop profiling activities and target advertising to finance its business as a result of the joint action by the Consumer Protection Cooperation Network (a pan-European enforcement network bringing together national consumer authorities).[73]

Even though consumer law thus does not limit data sharing as such, the Unfair Contract Terms Directive and the Unfair Commercial Practices Directive help to protect consumers by requiring transparency about the use of data in consumer contracts and by banning certain unfair commercial practices.

3. Enablers of data sharing

While competition, personal data protection and consumer law potentially limit data sharing, these regimes also enable data sharing. Indeed, competition law might impose the access to data under the essential facilities doctrine or as an antitrust remedy to ensure a level playing field. Moreover, personal data protection law enables data sharing via the right to data portability enshrined in Article 20 of the GDPR. Additionally, consumer law also enables data sharing as the underlying idea of Article 16 of the Digital Content Directive[74] is to allow the consumers to retrieve their data from traders who provide them with digital content and digital services, in order to then share this data with other traders.

3.1. Access to data under Article 102 TFEU and the essential facilities doctrine

3.1.1. Cases so far

Among the essential facilities cases reviewed in Section 2, three are information-related. In *Magill*, the Court of Justice validated the compulsory access to programme listings, data for which there was a legal barrier (the copyright) and which was a by-product of the main activities of the broadcasters. In *IMS*, the Court of Justice set the conditions to impose access to a structure for data which was a *de facto* industry standard. In *Microsoft*, the General Court validated the compulsory access to interoperability information which were also close to *de facto* industry standard.

Next to those EU cases, two non-digital national cases, which are very similar, are interesting. In both cases, a firm uses a customer list developed when it enjoyed a legal monopoly to promote a new service allowing it to compete unfairly through data cross-subsidisation which "un-levels" the playing field between the former monopolist and the new entrants. The first case was decided by the French competition authority against the previous gas monopolist *Gaz de France* (now Engie) which was using its customers list to promote a new gas service. In an interim decision, the authority forced Gaz de France to share the list with its competitors on the gas market as such a database was developed under a legal monopoly and was not easily reproducible by new entrants.[75] In the final decision, the authority imposed a fine of € 100 million on GDF.[76] The second case was decided by the Belgian competition authority against the National Lottery which was using its customers lists to send a one-off promotional email to launch its new sports betting product.[77] Given its nature and size, the authority concluded that the contact details could not have been

[73] Press release European Commission, 'Facebook changes its terms and clarify its use of data for consumers following discussions with the European Commission and consumer authorities', 9 April 2019, available at https://europa.eu/rapid/press-release_IP-19-2048_en.htm.
[74] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.
[75] Decision 14-MC-02 of 9 September 2014 of the French Competition Authority, *Direct Energie and UFC Que Choisir v. Engie*. This decision is based on the opinion that the French competition authority had adopted in 2010: Opinion 10-A-13 of the French Competition Authority of 14 June 2010 on cross-use of customers database.
[76] Decision 17-D-06 of 31 March 2017 of the French Competition Authority, *Direct Energie and UFC Que Choisir v. Engie.*
[77] Decision 2015-P/K-27 of 22 September 2015 of the Belgian Competition Authority, *Stanleybet Belgium/Stanley International Betting and Sagevas/World Football Association/Samenwerkende Nevenmaatschappij Belgische PMU v. Nationale Loterij*.

reproduced by competitors in the market under reasonable financial conditions and within a reasonable period of time.[78]

In the digital sector, two American cases are also interesting. In both cases, a small firm was relying on the data of bigger digital platform to provide data analytics services and then, at some point, was cut off from the access to those data. In the first case, *PeopleBrowsr* analysed Twitter data to sell information about customer reactions to products or about Twitter influencers in certain communities. At some point, Twitter decided that its data will not anymore be accessible directly but should be bought from certified data resellers. Following a compliant by PeopleBrowsr, a Californian Court ordered, with interim measures, Twitter to continue to provide its data directly. Then the parties settled the case deciding that after a transition period, PeopleBrowser will get the data from the certified data resellers.[79] In the second case, *hiQ* analysed LinkedIn public available data to provide information to business about their workforces. At some point, LinkedIn had limited access to its data with legal and technical means because it wanted to provide similar services itself. Following a compliant by hiQ, a US federal district judge ordered LinkedIn to resume the supply of its data.[80]

3.2.2. Assessment of essential facilities conditions for data access

When applying the four conditions of the essential facilities doctrine to data, it is important to distinguish at which level of the big data value chain access is requested (raw data, structure, structured data, analysed data). This will determine the upstream market on which indispensability is assessed and the downstream market on which the elimination of competition and the emergence of a new product are assessed. It is also important to apply those conditions in the light of the characteristics of data mentioned earlier.

(i) Condition 1: Indispensability of data

When access to raw data is requested, assessment of the indispensability condition implies an enquiry as to whether an alternative raw dataset is available or could be collected by a firm having the same size as the data owner. Obviously, this is an empirical analysis that should be examined on a case-by-case basis.[81] The wide availability and the non-rivalry of data often do not make them indispensable as the Commission has concluded in several past merger cases.[82] However in some cases, data collection may be subject to legal, technical and economic barriers which may make them indispensable.[83] In addition, many collected data are often generated by the users themselves[84] which may facilitate finding of indispensability according to *IMS*. Finally, the fact that the requested data have not already been traded, which is very often the case in practice, should not be an obstacle to imposing sharing as, following *IMS*, it suffices that there is demand and that such demand can legally and practically be met.

When access is about data structure, the assessment of the indispensability condition implies an enquiry as to whether an alternative structure is available or could be built by a firm having the same size as the data structure owner. Again, this is an empirical issue, but data structuring may show important network effects and become a *de facto* industry standard as in *IMS*. Access may also be about structured data, i.e. the collected data and the structure. In this case, both assessments indicated are required.

---

[78] *Ibidem*, par. 69-70.
[79] http://blog.peoplebrowsr.com/2012/11/peoplebrowsr-wins-temporary-restraining-order-compelling-twitter-to-provide-firehose-access/ and http://blog.peoplebrowsr.com/2013/04/peoplebrowsr-and-twitter-settle-firehose-dispute/
[80] *HIQ Labs v. LinkedIn.*
[81] This is why the conclusion of Lambrecht and Tucker (2015) that big data is not a sustainable competitive advantage (which is a strategic management which is close to the essential facility concept in antitrust) is not convincing because it is too general.
[82] See Balto and Lane (2016), Lambrecht and Tucker (2015), Lerner (2014), Sokol and Comerford (2016).
[83] Also Drexl (2016:49), Ezrachi and Stucke (2016), Stucke and Grunes (2016).
[84] For instance, in the connected cars, most data are generated by the driver (Kerber, 2018b:328).

(ii) Condition 2: Elimination of effective competition in the downstream market

The assessment of the elimination of downstream competition is very complex in the case of big data for two reasons. First, the downstream market is not always known, as one of the main features of big data is to experiment, crunch a lot of data without knowing in advance what information or knowledge will be found and what action might be taken. Therefore, the refusal to share data may lead to the possible elimination of a competitor on a not-yet-defined and future market[85]. This requires a more dynamic analysis, better in line with market realities but more difficult to do and possibly increasing the risks of antitrust errors.

Second, the data owner is often not (yet) active on the downstream market because, as explained by Drexl (2016:49): 'a typical feature of the data economy is that data is collected for one purpose but may turn out to be interesting for very different purposes pursued by other firms of very different sectors.' As explained above, authors are divided on whether the second condition requires the presence of the data owner on the downstream market and the case law is not clear. Given the firms' strategies and the competitive dynamics in the data economy, not requiring the presence of the data owner on the downstream market is suggested. The evolution of digital industries is quick and uncertain, and many firms are "paranoid" about the next disruptive innovation.[86] Thus, a data owner may refuse to share data with a firm that is not (yet) a competitor either because it plans to enter in the downstream market (future offensive leverage) or because it fears that the data seeker will disrupt its business (defensive leverage). In short, given the characteristics of the data economy, refusal to deal while not being active on the downstream market is not necessarily exploitative and may well be exclusionary. Again, much more dynamic analysis would be better aligned with market realities but would be difficult to do.

(iii) Condition 3: New product and consumer harm

As explained above, the interpretation of this condition is not very clear. The European Courts link this condition to the protection of the facility by an intellectual property right but have applied it more strictly in some cases than in others. The Commission integrates this condition into a more general consumer harm assessment.

Taking the Courts interpretation, the first issue is thus to determine whether the data to which access is required are protected by IP rights. That will depend, among other things, on the level in the value chain at which access is required. If there is IP protection, the next issue is whether the product that the access seeker aims to bring on the downstream market is sufficiently new or, at least improved, compared to the data owner's products. Drexl (2016:52) is doubtful that that will often be the case as he considers that the generation of new information thanks to data sharing is often not sufficiently innovative to justify the compulsory licensing of the intellectual property right.

However, more fundamentally, the assessment of this condition faces the same two difficulties analysed previously for the second condition, i.e. the product to be offered by the access seeker is often still unknown and the facility owner is often not (yet) providing a competing product. Therefore, the more general consumer harm approach proposed by the Commission is more appropriate to the characteristics of the data economy. Thus, the competition authority will have to examine whether, for consumers, the likely negative

[85] Keber (2018b:321) shows, in the context of connected cars, that the uncertainty on the future use of data also make difficult the reliance of the aftermarket theory.

[86] Andy Grove, the iconic founder of Intel, wrote in 1999 a book that he famously titled: Only the paranoid will survive. On disruptive innovation, see Gans (2016).

consequences of the refusal to share data outweigh, over time, the negative consequences of imposing data sharing.[87]

(iv) Condition 4: No objective justification and efficiencies

The last condition covers the economic and non-economic defence that the dominant data owner may oppose to compulsory data sharing. The data owner could show that compulsory sharing would undermine its incentives to collect, structure or analyse data (depending on the level at which the access is required). As investment increases going down the big data value chain, the lower level the access is required, the more investment incentives need to be protected. As already explained, this justification is connected to main cost-benefit analysis at the basis of imposing duty to deal. The data owner could also show that compulsory sharing would violate some privacy laws (which may be the case if personal data were to be shared), undermine safety or security (which may be the case for financial data or data related to connected cars),[88] or not be technically possible. For all those justifications, a proportionality test needs to be applied.

Thus, the four conditions of the essential facilities should be applied considering the characteristics of the data and the competitive dynamics of the data economy. In some circumstances, they may be fulfilled and justify an antitrust compulsory data sharing order. However, those conditions are sufficient but not necessary to prove the exceptional circumstances justifying the imposition of a duty to deal under Article 102 TFEU. They are merely proxies for the fundamental cost-benefit analysis described below.

(v) Balancing interests with data

The key issue is to determine whether the benefits of compulsory data sharing outweigh its costs.[89] The benefits are created by the entry of the data access seeker that may bring more competition, follow-on or breakthrough innovation, diversity and choice to the secondary market. The costs are the reduced investment incentives for the facility owner and for the potential access seeker and the operation costs of the antitrust enforcers and the dominant firms that have to implement the access obligations.

Those benefits and costs largely depend on the characteristics of data. The benefits of data sharing may be higher than for other (single-purpose) inputs because data are general-purpose and may be used and re-used in several contexts to build different information and knowledge.[90] Conversely, the costs of data sharing on investment incentives may be lower than for other (rival) inputs because data are non-rivalrous and the data owner may keep them while sharing them, hence its incentives to collect, structure or analyse them remain unchanged. Such incentive costs may even be zero when the data were obtained as by-product of another activity done independently of the data collection, as was the case in *Magill*.[91] In this hypothesis, the value of the data amounts to a windfall gain for its owner. The incentive costs will also be reduced when the data were constituted under the protection of a legal monopoly as in *Gaz de France* or in the *Belgian National Lottery*.[92]

The cost and benefit analysis also depend on the competitive dynamics in the data economy. Data markets show important economies of scale and scope on the supply side and massive direct and indirect network

[87] To paraphrase para 86 of the Priorities Guidance.
[88] Kerber (2018b:318-319).
[89] Kerber (2018b).
[90] Also Abrahamson (2014:879)
[91] Graef (2016), Prufer and Schottmuller (2017), Rubinfeld and Gal (2017:377); Schweitzer et al. (2018).
[92] In those two national cases, we may also claim that the customers list was also a by-product to the core activities of the data owner.

effects on the demand side.[93] This leads the markets to tip more often than in other sectors of the economy, which implies that competition enforcement should focus on preserving the contestability of those market for which data sharing may be key. Data markets also show rapid and uncertain innovation often after extensive experimentation. This requires better understanding of the firms' strategies that may for instance terminate data sharing to free ride on the experimentation costs or refuse to share data to alleviate the risks of future disruption.

Therefore, applying the *same* cost-benefit analysis which is at the core of the antitrust case-law of duty to deal in light of the *different* characteristics of data and the competitive strategies and dynamics of the data economy, leads us to suggest that the threshold for imposing data sharing under Article 102 TFEU should be lower than the threshold to impose access to other products.[94] However, lower threshold does not mean no threshold, as the freedom to contract and right of propriety still need to be protected in the data economy. As in the other sectors of the economy, the antitrust agency should convincingly demonstrate that the benefits of sharing data outweigh its costs.

3.2. Data sharing as antitrust remedy to ensure a level playing field

In the previous section, we have discussed how the combination of data through a merger can lead to competition concerns and thereby limit data sharing when a remedy would require the merging parties to keep their datasets separate. Interestingly, merger review can at the same time be used to impose remedies that would enable data sharing for the same reason of addressing the competition concerns arising from a merger. Indeed, when the level of data concentration enabled by a merger significantly impedes effective competition, two types of approaches can be taken. To address the competition concerns, either the datasets involved are to be kept separate, which limits data sharing among the merged parties, or the data is to be divested to a third party, which would enable data sharing beyond the merging parties. The reasoning behind the latter approach is that by requiring the merging parties to divest or even duplicate the relevant data, competitors are to develop competing or complementary services so to keep the relevant market competitive after the merger.[95] Precedent for such a remedy can be found in the context of the acquisition of Reuters by Thomson in 2008 where the Commission approved the merger on the condition that the merging parties would divest copies of their databases containing financial information.[96]

Beyond cases where refusals to give access to data amount to abuse of dominance (as analysed in the sub-section above), other types of abuses may also be addressed by imposing remedies that enable data sharing. The 2019 report on 'Competition policy for the digital era' written by the three experts appointed by Competition Commissioner Vestager suggested data access as a restorative remedy in cases of self-preferencing.[97] Self-preferencing is behaviour whereby a dominant firm gives more favourable treatment or more prominence to its own affiliated services versus those of rivals. A question is whether requiring a dominant firm to discontinue the abusive self-preferencing is sufficient to restore effective competition in the relevant market, considering that the self-preferencing has significantly benefited the market position the dominant firm's service in relation to competitors. As examples of restorative remedies that would allow disadvantaged competitors to regain strength, the experts refer to the possibility of giving competitors "*access to the dominant platform's competitively relevant data resources or otherwise compensate for their*

[93] As explained in Bourreau and de Streel (2019), such characteristics of the data markets amplify the pro and anti-competitive effects of firms' behaviours such as refusal to share.
[94] Also calling for lower threshold, Abrahamson (2014), Kerber (2018:328), Meadows (2015); Schweitzer et al. (2018). OECD (2015) goes also in the same direction.
[95] N.-P. SCHEPP AND A. WAMBACH, "On Big Data and Its Relevance for Market Power Assessment", *Journal of European Competition Law & Practice* 2016, vol. 7, no. 2, (120), p. 123.
[96] Case COMP/M.4726 – *Thomson Corporation/Reuters Group*, 19 February 2008.
[97] Crémer, de Montjoye and Schweitzer (2019:68).

reduced visibility or lack of data access in the past".[98] As a result, remedies that will enable data sharing can also be imposed in the context of other types of abuse of dominance cases beyond refusals to give access to data when the identified competition concerns can be addressed through mandatory data sharing. This includes the sharing or provision of access to data by the dominant firm to competitors but also to consumers. For instance, one can envisage a competition authority imposing a remedy to enable data portability (to which the attention turns in the next section) in an effort to address an exploitative abuse consisting of the excessive extraction of personal data from consumers.[99]

3.3. Right to data portability in the GDPR

One of the novelties of the GDPR has been the introduction of a data portability right in its Article 20. The goal of this right is to strengthen the "data subject empowerment", i.e. the power of control that the data subjects have on their own personal data.[100] To do so, Article 20.1 of the GDPR provides that the data subjects shall have the right to receive the personal data concerning them, which they have provided to a controller (the original controller), in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller (the recipient controller) without hindrance from the original controller. For instance, the data subject should have the possibility to extract his list of contacts from his webmail application in order to build a wedding invitation list that he can then share with his wedding planner.[101] The scope of this right is however limited to specific categories of personal data processing and to certain specific categories of personal data.

Data subjects can only call upon their data portability right for processing carried out by automated means, and which are based either on the data subjects' consent or are necessary for the performance of a contract.[102] There is thus no general right to data portability, since this right does not apply to processing operations necessary for the performance of a task in the public interest vested in the controller, nor to processing operations necessary for the compliance with a legal obligation to which the controller is subject.[103] For instance, a financial institution has no obligation to respond to a portability request relating to personal data that has been collected in the context of the compliance with its legal obligation to fight money laundering.[104]

Moreover, data portability does not allow sharing all types of personal data, but only the personal data "provided" by the data subject to the original controller. According to the Article 29 Working Party guidelines (which are not legally binding but have an authoritative status), "provided" personal data are "*data actively and knowingly provided by the data subject*"[105] (name, age, email address…) and "*observed data provided by the data subject by virtue of the use of the service or the device* [of the data controller]"[106] (search history, traffic and localisation data, number of steps walked during the day…).[107] However, in the view of the Article 29 Working Party, personal data cannot be considered as "provided" if it involves "*inferred data and derived data (…) created by the data controller on the basis of the data provided by the*

[98] Ibidem.
[99] Costa-Cabral (2016: 511)
[100] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.
[101] *Ibid*., p. 5.
[102] Article 20.1 of the GDPR.
[103] Article 20.3 and Recital 68 of the GDPR.
[104] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 8.
[105] *Ibid*., p. 10.
[106] *Ibidem*.
[107] The inclusion of these observed data in the scope of the "provided" data is criticised by some. See D. Meyer, "European Commission experts uneasy over WP29 data portability interpretation", 25 April 2017, available at https://iapp.org/news/a/european-commission-experts-uneasy-over-wp29-data-portability-interpretation-1/.

data subject"[108] (user profiles, results of an evaluation of the data subject's health based on the data collected by his smart watch…).
Article 20.2 of the GDPR goes a step further in terms of enabling data sharing as it provides that the data subject shall have the right to have the personal data transmitted directly from one controller to another. In essence, this means that the recipient controller can port data directly from the original controller's system, provided that the data subject has consented to this operation. Therefore, the data does not have to transit through the data subject's IT system. However, Article 20.2 of the GDPR only applies "*where technically feasible*", which means that the original controllers have no obligation to ensure this technical feasibility, thus limiting this provision's efficiency in practice. In this regard, it should be noted that Google, Facebook, Microsoft and Twitter contribute, with other actors, to the *Data Transfer Project*, launched in 2017, which aims at creating an open source platform allowing the direct portability of data between the participating data controllers.[109]

Additionally, it should be pointed out that the Second Payment Service Directive[110] (hereafter "PSD2") provides for a sector-specific application of Article 20.2 of the GDPR.[111] Indeed, PSD2 gives the right to providers of payment initiation service and providers of account information service[112] to have access to the payment account information[113] of the users of their services (the consumers), if the latter have explicitly consented to such access.[114] This constitutes a sector-specific application of Article 20.2 of the GDPR, as it compels the banks (original controllers) to make this direct transmission of the data subjects' personal banking information to recipient controllers "technically feasible*"*. This is the main difference with Article 20.2 of the GDPR, which contains no such technical feasibility obligation. At the same time, the scope of the access mandated by the PSD2 is limited to the two scenarios of payment initiation and account information, whereas the GDPR's data portability right applies generally irrespective of the type of service for which the data will be used.

3.4. Data retrieval under the Digital Content Directive

Like competition and personal data protection law, consumer law also enables data sharing, notably through the means of Article 16 of the Digital Content Directive.[115] This provision allows consumers to retrieve some of the data they have provided to a trader[116]. More specifically, this Directive provides that, in the event of the termination of the contract, the trader shall, at the request of the consumer, make available to the consumer any content other than personal data, which was provided or created by the consumer when using the digital content or digital service supplied by the trader.[117] The consumer shall be entitled to

[108] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10.
[109] See https://datatransferproject.dev/.
[110] Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, , *OJ L 337/35*, 23 December 2015.
[111] Colangelo and Borgogno (2018:3); Vezzoso (2018:12-13).
[112] Respectively defined as "*a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider*" and as "*an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider*" (Articles 4.15 and 4.16 of the Directive 2015/2366).
[113] Defined as "*account held in the name of one or more payment service users which is used for the execution of payment transactions*" (Article 4.12 of the Directive 2015/2366).
[114] Articles 64 to 67 of the Directive 2015/2366.
[115] Directive 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, *OJ L 136/1*, 22 May 2019.
[116] A trader is defined as "*Any natural or legal person, irrespective of whether privately or publicly owned, that is acting, including through any other person acting in that natural or legal person's name or on that person's behalf, for purposes relating to that person's trade, business, craft, or profession, in relation to contracts covered by this Directive*" (Article 2.5 of the Directive 2019/770).
[117] Article 16.4, al. 1 of the Directive 2019/770.

retrieve that digital content free of charge, without hindrance from the trader, within a reasonable time and in a commonly used and machine-readable format.[118]

The Directive therefore grants a form of portability right for the non-personal data provided or created by the consumer. However, this right for consumers, or duty imposed on traders, does not apply in a number of situations, namely where data: (1) has no utility outside the context of the digital content or digital service supplied by the trader; (2) only relates to the consumer's activity when using the digital content or digital service supplied by the trader; or (3) has been aggregated with other data by the trader and cannot be disaggregated or only with disproportionate efforts.[119] These exceptions are justified by the fact that, in those cases, the content is of little practical use to the consumer, who therefore has a limited interest in the portability of such data, particularly in view of the fact that requiring such a mechanism is costly for the trader.[120]

Yet, the Directive is only an indirect enabler of data sharing as it solely provides the consumer with a right to retrieve some of its non-personal data. It does not allow the direct transmission of data between two traders. Nevertheless, the underlying idea of the Directive is to allow the consumers to retrieve their data in order to then share this data with other traders. Indeed, the proposal at the origin of the Directive outlined that, in order to promote competition, it is necessary to ensure that consumers can easily switch content providers, by reducing legal, technical and practical obstacles, such as the inability to recover all the data that the consumer has produced or generated through his use of digital content.[121] This is because the consumer could be deterred from terminating a contract for digital content or a digital service if he cannot recover access to the content in question as a result of such termination.[122]

4. Analytical framework for data sharing

After having presented the dual relationship that competition, personal data protection and consumer law have with data sharing, this paper will now draw an analytical framework for data sharing by outlining how these regimes complement each other, on the one hand, and by outlining the tensions within and between these regimes, on the other hand.

4.1. Complementarity between the regimes

While competition, personal data protection and consumer law have their own objectives, they complement one another as the effects or outcomes of one regime can further the goals of another regime. This is apparent from the fact that competition law potentially limits data sharing, which furthers the goals of the personal data protection principles of purpose limitation and data minimisation. This is also apparent from the fact that, to some extent, the data retrieval right under the Digital Content Directive complements and aligns with the GDPR's right to data portability.

4.1.1. Competition law potentially limits data sharing, furthering the goals of personal data protection

Competition law can stand in the way of data sharing when the exchange of data leads to collusion under Article 101 TFEU or gives rise to competition concerns under merger review due to the combination of the datasets of the merging parties. In such cases, the application of competition law at the same time will further compliance with data protection law. When data is kept separate in order to prevent collusion under

[118] Article 16.4, al. 2 of the Directive 2019/770.
[119] Articles 16.3 and 16.4, al. 1 of the Directive 2019/770.
[120] Recital 71 of the Directive 2019/770.
[121] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634, p. 22.
[122] Recital 70 of the Directive 2019/770.

Article 101 TFEU or to address a significant impediment to effective competition under merger review, this also prevents data processing from running counter to the data protection principles of data minimisation and purpose limitation. Competition law is then applied to protect economic efficiency and at the same time achieves results that foster data protection considerations as well.

This interaction of competition law with data protection law also works the other way around. By imposing restrictions on the extent to which personal data can be combined or exchanged, the GDPR can act as a limit restricting the room for anticompetitive effects to arise. Such a reasoning came up in the *Microsoft/LinkedIn* merger decision where the Commission explained that Microsoft is subject to EU data protection rules that limit "*its ability to undertake any treatment of LinkedIn full data*".[123] As such, the reliance on data protection law was one of the elements in the Commission's reasoning concluding that the combination of the datasets of the two merging parties did not raise competition concerns. Although it is a welcome development that the Commission integrates data protection law into its competition assessment to let the regimes complement each other's effects, a cautious approach is necessary to make sure that the data protection rules relied upon are indeed capable of restricting the scope for market players to engage in anticompetitive conduct.[124]

4.1.2. Alignment of the data retrieval right under the Digital Content Directive with the GDPR's data portability right

To some extent, the data retrieval right contained in Article 16.4 of the Digital Content Directive (DCD) aligns with the data portability right contained in Article 20 of the GDPR. This is apparent from a comparison of the two provisions.[125] Apart from the application of these data protection and consumer law instruments, one should also keep in mind that competition law can also facilitate data portability.[126]

(i) Objectives

The goal of the data portability right in the GDPR is to strengthen the "data subject empowerment", i.e. the power of control that the data subjects have on their own personal data.[127] This "data subject empowerment" objective is translated into two sub-objectives.

On the one hand, in a strict conception of the notion of "data subject empowerment", this right to data portability in the GDPR "*represents an opportunity to "re-balance" the relationship between data subject and data controllers*", and this, "*by affirming individuals' personal rights and control over the personal data concerning them*".[128] This is an undeniable point in common with the DCD, as the "data subject empowerment" objective of the GDPR is part of the broader "consumer empowerment", which is the central objective of consumer protection law.[129]
On the other hand, and in a broader conception of the notion of "data subject empowerment", this right to data portability in the GDPR should make it easier for the data subject to change service providers.[130] Once again, this objective transpires in the DCD, as its goal is to ensure that consumers can easily switch content providers, by recovering all the data that the consumer has produced or generated through his use of digital

[123] Case M.8124 – *Microsoft/LinkedIn*, 6 December 2016, par. 255.
[124] For a further discussion, see Graef, Clifford and Valcke (2018: 215-217).
[125] See, inter alia, Metzger, Efroni, Mischau & Metzger (2018:102-105); Graef, Husovec, and Purtova (2018); Ledger and Tombal (2018).
[126] For a discussion, see: Lynskey (2017:793-814) and Van der Auwermeulen (2017:57-72).
[127] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.
[128] *Ibidem*.
[129] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634, p. 3.
[130] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 4.

content.[131] The GDPR and the DCD thus share a clear common objective, namely to prevent consumers from being "locked-in" the services of Internet giants, such as Facebook or Google.

(ii) Scope of application

While Article 20 of the GDPR applies to personal data that has been "provided"[132] by the data subject, Article 16.4 of the Digital Content Directive applies to any content *other than personal data*, which was provided or created by the consumer when using the digital content or digital service supplied by the trader (emphasis added). The scope of application of the DCD is thus complementary to that of the GDPR. This is explicitly stated in the text of the DCD, which provides that the trader remains bound by the obligations of the GDPR[133], which prevails over this Directive in the event of a conflict of provisions.[134] It therefore seems that the objective of the final text of this Directive is to avoid any overlap with the regime of Article 20 of the GDPR.[135]

However, this distinction between personal and non-personal data might be problematic in practice. Indeed, given the GDPR's broad definition of this concept, namely "*any information relating to an identified or identifiable natural person*"[136], the vast majority of the data provided or created by the consumer may likely be considered as personal data. In any case, it should be underlined that the "inferred and derived" personal data, which are not considered as data "provided" by the data subject, are neither covered by the GDPR nor by the DCD, and thus cannot be ported.

(iii) Data recipients

While Article 20.1 of the GDPR provides that the data subject has the right to receive the personal data which he has provided to a controller and to transmit it to another controller without hindrance, Article 20.2 of the GDPR provides that the data subject also has the right to have the personal data transmitted directly from one controller to another, "*where technically feasible*". The DCD, on the other hand, does not allow this direct transmission, since it only aims to establish the consumer's right to recover the data personally.[137] In this sense, it is closer to the right of access contained in the GDPR, which allows a data subject to obtain a copy of his personal data.[138] In the event that the consumer wishes to share data with a third party, the mechanism of the DCD is therefore less effective than the right to data portability of Article 20 of the GDPR.

(iv) Data formats

Article 20 of the GDPR states that the ported data have to be provided in a structured, commonly used and machine-readable format. As a welcome development, the format requirements contained in the final text

[131] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634, p. 22.
[132] Are considered as "provided" the "*data actively and knowingly provided by the data subject*" and the "*observed data provided by the data subject by virtue of the use of the service or the device* [of the data controller]", but not the "*inferred data and derived data (…) created by the data controller on the basis of the data provided by the data subject*" (Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 10).
[133] Article 16.2 of the Directive 2019/770.
[134] Article 3.8 of the Directive 2019/770.
[135] On the contrary, the proposal at the origin of the Directive targeted "*all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content*" (Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634, Articles 13.2.c) and 16.4.b)). This wording also covered personal data and thus overlapped, to some extent, with the GDPR.
[136] Article 4.1 of the GDPR.
[137] Article 16.4 of the Directive 2019/770.
[138] Article 15.3 of the GDPR.

of the DCD have been aligned with those provided for in the GDPR, as the data must be returned to the consumer "*in a commonly used and machine-readable format*".[139] This was not the case in the proposal at the origin of the Directive, which had less stringent data format requirements than Article 20 of the GDPR, as this initial text provided that the data had to be returned to the consumer in a "*commonly used data format*".[140] In this sense, the proposal was closer to the format requirement for the right of access in the GDPR, according to which the data had to be delivered in a "*commonly used electronic form*".[141]

(v) Consequences of the exercise of the right and the temporality of requests

The exercise of the right to data portability does not automatically imply an obligation for the controller to erase the ported data.[142] Accordingly, when Article 20.1 of the GDPR indicates that the data subject has the right to receive the personal data he has provided to the controller, this should be understood as meaning that the data subject has a right to receive a "copy" of this data. Moreover, the data subject can exercise his portability right several times towards the same data controller, notably in order to port the data that has been updated by the controller (who can continue to use the data) since the last portability request. Unlike Article 20 of the GDPR, the DCD provides that, when the consumer terminates the contract, the trader must refrain from using the non-personal data provided or created by the consumer.[143] The fate of the data held by the original controller/trader therefore differs in the two regimes, as Article 20 of the GDPR does not prevent the original controller from continuing to use the ported data, while the DCD provides that the trader must refrain from using the data in the future unless it has been generated jointly by the consumer and others, and other consumers are able to continue to make use of the content.[144] In reality, this difference can be explained by the fact that data can be ported at any time under the GDPR, while data portability is only made possible after the termination of the contract by the consumer in the DCD.

(vi) Cost and deadline to process the requests

The data controller may not request any payment from the data subject exercising his right to data portability under Article 20 of the GDPR, unless the data subject's request is manifestly unfounded or excessive, in particular because of its repetitive character. In such cases, the controller may either charge a reasonable fee based on the administrative costs incurred or even refuse to implement the request altogether.[145] Moreover, it must act on a data portability request without undue delay and in any event within one month of the receipt of the request, except in more complex cases, where the maximum response time is three months.[146] Similar to the GDPR but leaving no room for traders to charge a fee or refuse to act, the DCD provides that the consumer shall be entitled to retrieve the data free of charge.[147] Regarding the deadline to reply to the request, the DCD only provides that the data should be given to the consumer "*within a reasonable time*" after the termination of the contract.[148] While the DCD does not provide any further information as to how these terms must be interpreted, the deadline of one month provided for in the GDPR could arguably be used to assess this "reasonable" character, in order to align these two regimes.

---

[139] Article 16.4 of the Directive 2019/770.
[140] Proposal for a Directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content, 9 December 2015, COM(2015) 634, Articles 13.2.c) and 16.4.b).
[141] Article 15.3 of the GDPR.
[142] Article 20.3 of the GDPR.
[143] Article 16.3 of the Directive 2019/770. The only exceptions are if the data has no use outside the context of the content or service; if the data only relates to the consumer's activity when using the content or service; if the data has been aggregated with other data by the trader and cannot be disaggregated or can only be disaggregated with disproportionate effort; or if the data has been generated jointly by the consumer and other persons who continue to use them (Article 16.3 of the Directive 2019/770).
[144] Article 16.3.d) of the Directive 2019/770.
[145] Article 12.5 of the GDPR.
[146] Article 12.3 of the GDPR.
[147] Article 16.4 of the Directive 2019/770.
[148] Article 16.4 of the Directive 2019/770.

(vii) Summary

In light of the above, it appears that, to some extent, the regimes of the GDPR and the DCD are complementary and align. Indeed, these regimes share a clear common objective and have complementary scopes of application. Moreover, they are aligned in terms of costs and deadline to process the request, and in terms of format requirements. However, these regimes diverge when it comes to the data recipients and to the consequences of the exercise of the right and the temporality of requests. It is thus clear that the European legislator has attempted to align the two regimes as much as possible, in order to avoid complex situations of portability overlap, which could have led to legal uncertainties.

4.2. Tensions within regimes

As competition, personal data protection and consumer law have a dual relationship with data sharing, by both limiting and stimulating data sharing, this leads to tensions within regimes. Indeed, while competition law can mandate data sharing to address competition concerns, data sharing might also facilitate collusion. Moreover, the principles of purpose limitation and data minimisation in personal data protection law limit data sharing, while the data portability right promotes the exchange and reuse of data.

4.2.1. Competition law can mandate data sharing but data sharing can at the same time entail competition concerns

The tension within the field of competition law relates to the fact that data sharing can be necessary as a remedy to address competition concerns under abuse of dominance or merger review, but at the same time may create concerns of collusion under Article 101 TFEU. In the context of refusals to deal, this dilemma is well-know. The US Supreme Court judgment in *Trinko* made clear that liability for refusals to deal under US antitrust law is very limited. In this context, Justice Scalia famously wrote that: "*Enforced sharing also requires antitrust courts to act as central planners, identifying the proper price, quantity, and other terms of dealing–a role for which they are ill-suited. Moreover, compelling negotiation between competitors may facilitate the supreme evil of antitrust: collusion*".[149] The concern is that once a competition authority or court obliges a dominant firm to give access to an input to address abusive behaviour, this would require the dominant firm to negotiate with access seekers about the price and other conditions of access. Such negotiations could give rise to new competition concerns, namely in the area of collusion. Another issue specific to data sharing as a competition law remedy is that the exchange of data by the dominant firm should not include commercially sensitive information. Otherwise, a competition problem under Article 102 TFEU would be addressed by adopting a remedy that potentially directly violates Article 101 TFEU. The same reasoning applies to a divestiture of data as a remedy under merger review, which could similarly create concerns about collusion between the merged entity and third parties.

The tension between the requirements of Articles 101 and 102 TFEU also becomes visible in the ongoing *Amazon* investigation of the Commission. The competition concern in the case relates to the collection by Amazon of transaction data from downstream retailers on the basis of Amazon's standard agreements with these retailers and the way Amazon can use this data to improve its own business activities as a retailer. This means that the case can either be constructed as a potential violation of Article 101 TFEU, when the agreements involve the exchange of commercially sensitive information by the retailers to Amazon, or a potential breach of Article 102 TFEU, when Amazon is considered to abuse its dominance, for instance, by using the third party transaction data to shut out retailers through offering popular products to consumers at a lower price. The only remedy to address possible collusion concerns would be to force Amazon to

[149] *Verizon Communications v. Law Offices of Curtis V. Trinko, LLP* (*Trinko*), 540 U.S. 398 (2004), at 408.

discontinue the exchange of data from retailers, which would thus limit data sharing. Such a remedy can also address the possible abuse of dominance concerns. By requiring Amazon to refrain from using third party transaction data for its own downstream retail activities, a level playing field is created between Amazon and the independent retailers. An alternative remedy to resolve the abuse of dominance would be to require Amazon to share the transaction data among all independent retailers. This approach would also result into a level playing field, as Amazon would no longer have a competitive advantage vis-à-vis retailers in terms of the insights about the transactions being concluded on its marketplace. Data sharing as a remedy could arguably even create a more competitive market due to increased levels of transparency about the available offerings on Amazon's marketplace. At the same time, one should prevent that such a remedy facilitates collusion among retailers. This creates a dilemma where data sharing can have both beneficial and detrimental effects to competition.

To resolve this tension between the requirements of separate branches of competition law, data sharing as a remedy to address competition concerns under abuse of dominance or merger review should not go as far as to result into the exchange of commercially sensitive information. However, as discussed in section 2 above in the context of data pooling, the boundaries of liability for data sharing under Article 101 TFEU may not be easy to draw in practice.

4.2.2. Tensions between the principles of purpose limitation and data minimisation and the right to data portability in the GDPR

Tensions can also appear within the GDPR, as its principles of purpose limitation[150] and data minimisation[151] limit data sharing, while the personal data portability right[152] promotes the exchange and reuse of data. Opinions may differ on the extent to which the relationship between these notions qualifies as a tension. On the one hand, the right to data portability arguably fits the fundamental rights nature of data protection by enhancing the control of the data subject over his or her personal data[153] so that from the perspective of the relationship between an individual data subject and a data controller no tension occurs. On the other hand, ported data can also relate to other individuals and leads to the duplication of personal data to other controllers so that a tension occurs from the perspective of the broader impact on the data economy. In practice, this means that these two principles have to be considered when implementing the data portability right. This articulation will essentially have to be done prior to the porting of the data.

Indeed, the Working Party 29 recommends that the recipient controller should inform the data subjects about the purposes for which the ported data will be processed and about the categories of personal data that are adequate, relevant and necessary for these purposes, in order to prevent a breach of these purpose limitation and data minimisation principles.[154] Moreover, if the recipient controller realises that the data subject has ported more data than what is necessary for the purpose he is pursuing, he will have to delete this excessive data as soon as possible, in order to avoid any liability issue.[155] This clarifies one of the uncertainties faced by the original controllers regarding the right to data portability, namely whether there is a risk that they might be found liable for the unlawful processing of the ported data made by the recipient controller, notably because of a breach of these purpose limitation and data minimisation principles. This uncertainty stems from the fact that the GDPR does not tackle this issue. Consistently with what has been outlined above about the recipient controller, the Working Party 29 has indicated that insofar as the original controller responds to the request for portability in compliance with the conditions of Article 20 of the GDPR, it should not be held liable as a result of the processing carried out on the data by the recipient

[150] Article 5.1.b) of the GDPR.
[151] Article 5.1.c) of the GDPR.
[152] Article 20 of the GDPR.
[153] Lynskey (2017:793-814).
[154] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 13.
[155] *Ibidem*.

controller.[156] Indeed, the original controller acts here on behalf of the data subject, and should not be responsible for any later infringement potentially committed by the recipient controller. Nevertheless, according to the Working Party 29, the original controller should still set up certain safeguards, such as internal procedures to ensure that the data that is actually transmitted matches the data whose portability is requested, in light of the purpose limitation and data minimisation principles.[157]

These two principles will also have to be considered in order to limit the porting of personal data from other data subjects than the one exercising his data portability right. This limitation to the scope of the data sharing has been integrated in the provision pertaining to the data portability right, as Article 20.4 of the GDPR provides that this right needs to be articulated with the rights and freedoms of others, that it shall not affect. Accordingly, when a data subject exercises his right to data portability, it will be necessary to ensure that the personal data of other data subjects, who have not given their consent to such portability, are not transmitted, at the same time, to a recipient controller likely to process the personal data of such third parties.[158] Indeed, while the data subject at the origin of the portability request has given his consent to the recipient controller or has concluded a contract with him, this is not the case for the other data subjects whose data could be ported as a result of the exercise of this right. In this regard, the purpose limitation principle must not be overlooked. Given that the third parties in question have not consented to the transfer of their data to the recipient controller, this transfer can only take place if the purpose for which the transfer is made is compatible with the original controller's initial purpose of processing.[159] If this is not the case, the recipient controller will have to rely on a new lawful basis for the processing of these third parties' personal data, such as the "legitimate interests" basis of Article 6.1.f) of the GDPR.

In order to avoid such an issue, the Working Party 29 suggests that the processing of these other data subjects' personal data should be authorised only insofar as these data remain under the sole control of the data subject requesting the portability, and that they should only be processed for the purposes determined by this data subject.[160] The recipient controller could therefore not process these third parties' data for purposes that he has defined himself, such as prospecting purposes, as this would infringe the GDPR. Moreover, the recipient controller could not process these data for purposes that are not compatible with the purposes of the original controller. While being appealing in theory, this suggestion is nevertheless extremely restrictive and provides little interest for the recipient controller, whose margin of manoeuvre will be severely limited. However, the Working Party 29 makes another suggestion that is more interesting. It invites both the original and the recipient controllers to implement technical tools allowing the data subject to select the personal data he wishes to port, while excluding, where possible, the personal data of other data subjects.[161] This makes it possible to avoid, upstream, a potential infringement of the rights of these third parties. However, this is not sufficient in itself, as some personal data of third parties might necessarily have to be ported. Accordingly, in addition to these technical tools, it must also be reflected on the implementation of consent mechanisms for these other data subjects, in order to facilitate data portability.[162] Once again, the question will arise of the difficulty of implementing such a mechanism in practice. For example, in the banking sector, it would be practically impossible to obtain the consent of all the persons appearing in a list of banking transactions that a data subject would like to port to another bank.

4.3. Tensions between regimes: Compatibility with the GDPR of data sharing as a remedy to a competition law infringement

[156] *Ibid*., p. 6.
[157] *Ibidem*.
[158] *Ibid*., p. 11.
[159] Article 5.1.b) of the GDPR.
[160] Working Party 29, *Guidelines on the right to data portability*, WP 242 rev.01, 13 April 2017, p. 12.
[161] *Ibidem*.
[162] *Ibidem*.

Tensions do not only appear within regimes, but also between regimes, as the approach in one regime can cause clashes with the objectives of another one. Indeed, as outlined above, data sharing could be required by a competition authority in order to remedy a competition law infringement. Yet, one must not lose track of the fact that some of the data at hand could be personal data. This might, at first sight, seem to create tensions with the policy objective of the GDPR, as one of its aims is to provide more control to the data subjects on the personal data concerning them. Indeed, such a data sharing remedy might lead to the dissemination of such personal data, consequently reducing the data subjects' control on what happens with "their" data. Though some tensions might emerge between these two policy objectives, they are not incompatible, and sharing personal data can be beneficial for society, governments, undertakings and individuals.[163] The challenge is thus not whether one should prevail over the other, but rather how these policy objectives can be reconciled.[164]

Such data sharing remedy might come into conflict with the GDPR if the personal data is not anonymised prior to the transfer.[165] However, this might reduce the value of the dataset and, in any case, truly effective anonymisation is difficult to achieve.[166] In the vast majority of cases, the data will remain personal and the remedy will therefore have to comply with the rules of the GDPR. This requires, on the one hand, having a lawful basis for the data sharing, and, on the other hand, to comply with the general principles of personal data protection.

4.3.1. Lawful bases for the data sharing

According to the principle of separate justification, a remedy imposing data sharing would require a lawful basis at two levels, namely at level of the undertaking that holds the data and at the level of the undertaking that will receive the data, and these two lawful bases do not need to be the same.[167]

(i) Lawful bases for the data holder

Making the data available to a third party as a consequence of a remedy imposed by a competition authority amounts to a new processing for the data holder and is therefore in need of a lawful basis.[168] Arguably, three lawful bases could potentially be used by the data holder.

The first possibility would be to obtain the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision.[169] Indeed, obtaining a general consent *before* the decision will lack the specificity and explicitness required for the consent to be compliant with the GDPR.[170] The data holder will therefore have to seek the data subjects' consent to share the data with one or several specific recipients identified in the competition authority's decision.[171] However, it

[163] Information Commissioner's Office, "Data sharing code of practice – Draft code for consultation", 15 July 2019, https://ico.org.uk/media/2615361/data-sharing-code-for-public-consultation.pdf, p. 13.
[164] Muralidhar, Sarathy and Li (2014:2).
[165] J. Haucap, "A German approach to antitrust for digital platforms", in *Digital Platforms and Concentration - Second annual antitrust and competition conference*, S. Eyler-Driscoll, A. Schechter and C. Patiño (eds.), 2018, available at https://promarket.org/wp-content/uploads/2018/04/Digital-Platforms-and-Concentration.pdf, p. 12.
[166] Drexl (2018: 4). See also Wendehorst (2017:330-331).
[167] Wendehorst (2017:334-337).
[168] *Ibid*., p. 334-335.
[169] Articles 4.11 and 6.1.a) of the GDPR.
[170] Kathuria and Globocnik (2019: 27-28).
[171] *Ibid*., p. 28.

might be extremely complex and burdensome to do so in practice. The French *GDF Suez*[172] case, presented above, illustrates this point. The French *Autorité de la concurrence* found that GDF Suez had abused its dominant position in the market for natural gas and required GDF Suez to share certain customer information data with its competitors.[173] It ordered GDF Suez to inform the data subjects about the sharing of their data with their competitors and to give them the possibility to opt-out from this transfer.[174] Given that, at the time, the Data Protection Directive[175] was still in force and that this legislation was silent about whether such an opt-out solution was admissible, this seemed like an appropriate way to balance the personal data protection and competition considerations.[176] However, now that the GDPR is in force, requiring the data subjects to opt-out of the transfer, rather than to opt-in to the transfer, would no longer be GDPR-compliant, as, according to Article 4.11 of the GDPR, the data subject has to explicitly consent to the transfer.[177] This makes it much more cumbersome for the data holder and will surely affect the efficiency in practice of the data sharing remedy if the data holder relies on consent as a lawful basis for the transfer, as it is very likely that there will be fewer data subjects that opt-in than data subjects that do not opt-out.[178]

The second possibility would be to consider that the data sharing is necessary for the compliance with a legal obligation to which the data holder is subject.[179] The question here is whether a decision by a competition authority could qualify as such a legal obligation.[180] Indeed, Article 5.3 of the GDPR provides that the basis for the processing shall be laid down in Union law or Member State law. However, the word "law" is not defined anywhere in the GDPR. In that regard, the interpretation, by the European Court of Human Rights, of the requirement of the legality of an interference with a fundamental right[181] should be reminded. The Court consistently holds that the term "law" must not be given a "formal interpretation", which would necessarily imply the existence of a written statute having a legislative value, but rather a "material interpretation"[182], which not only covers the written statutes, but all the legal rules in force.[183] Indeed, the European Court of Human Rights has acknowledged that parliamentary proceedings, decisions, regulations or unwritten rules of law, such as case law decisions, could satisfy the requirement of legality.[184] Arguably, a similar interpretation could be given to the words "law" and "legal obligation" in the GDPR, and, accordingly, a competition authority's decision imposing data sharing could qualify as a "legal obligation".

The third possibility could be to argue that sharing the data is necessary for the purposes of the legitimate interests pursued by the data holder, and that these interests are not overridden by the interests or

---

[172] Autorité de la concurrence, Decision n°17-D-06 (*GDF Suez*), 21 March 2017, available at http://www.autoritedelaconcurrence.fr/pdf/avis/17d06.pdf.
[173] Graef (2016:271-272).
[174] Kathuria and J. Globocnik (2019:28).
[175] Directive 95/46 of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *OJ L 281*, 23 November 1995.
[176] *Ibidem*.
[177] *Ibidem*.
[178] *Ibid*., p. 28-29.
[179] Article 6.1.c) of the GDPR.
[180] On this issue, see Graef (2016:319); Kathuria and Globocnik (2019:21-22).
[181] *In casu* Article 8 of the European Convention on Human Rights (Right to respect for private and family life), in which personal data protection is rooted.
[182] E. Degrave, *L'E-Gouvernement et la protection de la vie privée. Légalité, transparence et contrôle*, Bruxelles, Larcier - Collection du CRIDS, 2014, p. 144.
[183] R. Ergec, *Protection européenne et internationale des droits de l'homme*, Bruxelles, Larcier, 2014, p. 232.
[184] ECtHR, *Sunday Times v. United Kingdom*, 26 April 1979, req. n°6538/74, §§ 46-53; ECtHR, *Hüvig v. France*, 24 April 1990, req. n°11105/84, § 28; ECtHR, *Kruslin v. France*, 24 April 1990, req. n°11801/85, § 29. See also P. De Hert, "Artikel 8. Recht op privacy", in *Handboek EVRM, Deel 2. Artikelsgewijze commentaar*, J. Vande Lanotte and Y. Haeck (eds.), Antwerp, Intersentia, 2004, p. 716.

fundamental rights and freedoms of the data subjects.[185] For the data holder, the legitimate interest could be that it has to comply with a competition authority's decision in order to avoid a potential substantial fine, but also that the data sharing would ensure a competitive environment that will benefit the consumers.[186] The key question is therefore whether the data holder's legitimate interest outweighs the data subjects' interests. As more undertakings will get access to their personal data due to the data sharing, this potentially reduces the data subjects' privacy. Moreover, it might also arguably increase the risks of de-anonymisation of other data, as making more data available increases the risk of re-identification through the "crossing" of information from various sources.[187] Accordingly, there might be cases where the legitimate interests of the data holder should not prevail over the data subjects' interests, and Article 6.1.f) of the GDPR should not be considered as a viable lawful basis for the data sharing remedy.

However, there are other cases where this data sharing might allow competitors to create privacy-oriented alternatives to existing services, which would benefit the data subjects in the long term. Indeed, the development of competitive alternatives is necessary to prevent data subjects from being "locked in" the services of the existing providers, as more switching possibilities would allow the data subjects to "penalise" more easily data controllers that violate (repeatedly) their privacy. Therefore, mandating data sharing might also, in certain situations, be beneficial for the data subjects as it will allow more privacy-oriented competition. In those cases, the legitimate interests of the data holder could prevail over the data subjects' interests – and might actually be aligned with these interests –, and accordingly the data sharing could be justified on the basis of Article 6.1.f) of the GDPR.

(ii) Lawful bases for the data recipient

While the data holder has to have a lawful basis to share data with the recipient, the data recipient also needs his own specific lawful basis for the processing that will be done once he has received the data.[188] Contrary to the data holder, the recipient should not be able to argue that this further processing is necessary for the compliance with a legal obligation to which he is subject. This is because, while the competition authority's decision to impose a data sharing remedy could arguably be considered as a legal obligation for the data holder that must comply with this decision, this decision does not impose any obligation on the data recipient to process the shared data. Therefore, the recipient cannot argue that he must necessarily process the data as a result of the competition authority's decision. Rather, he will have to rely on one of the other two lawful bases available to him, namely consent or the necessary processing for the purposes of the legitimate interests that he pursues.

The first basis for the data recipient could thus be the obtaining of the explicit freely given, specific, informed and unambiguous consent of the data subjects at hand *after* the competition authority's decision.[189] In this regard, what has been said above about consent as a lawful basis for the data holder can be transposed and will not be repeated.

The other possibility for the data recipient would be to argue that the data processing is necessary for the purposes of the legitimate interests that he pursues, and that these interests are not overridden by the interests or fundamental rights and freedoms of the data subjects.[190] For the data recipient, the legitimate interests would be the opportunity to offer (privacy-oriented) alternative products or services to the

[185] Article 6.1.f) of the GDPR.
[186] Kathuria and Globocnik (2019:25).
[187] *Ibid*., p. 26 and 32.
[188] Wendehorst (2017: 334-337).
[189] Articles 4.11 and 6.1.a) of the GDPR.
[190] Article 6.1.f) of the GDPR.

consumers, to restore competition on the market, and to reduce the data holder's competitive advantage.[191] Once again, the key question is therefore whether the data recipient's legitimate interests outweigh the data subjects' interests. In this regard, the above developments pertaining to the data holder can be transposed as well. There might thus be some cases where this further processing might allow competitors to create privacy-oriented alternatives to existing services, which would benefit the data subjects in the long term. In those cases, the legitimate interests of the data recipient could prevail over the data subjects' interests – and might be aligned with these interests –, and accordingly the data could be processed on the basis of Article 6.1.f) of the GDPR. To achieve this balancing exercise, the data recipient will need to be very specific about the use he will make of the shared data (e.g. which products or services he intends to offer thanks to the data, whether they are privacy-oriented or not, etc.), as this will allow to determine if this further processing would be harmful, or on the contrary beneficial, to the data subjects.

4.3.2. Compliance with the general principles of personal data protection

In order for data sharing as a remedy to be compatible with the data protection rules, the data holder and the data recipient must not only rely on a lawful basis for the processing, but they must also comply with the general principles of personal data protection. To do so, both the data holder and the data recipient will have to inform the data subjects about the personal data processing deriving from this data sharing remedy, in a fair and transparent manner.[192] On the one hand, the data holder will have to inform the data subjects that it has been compelled by a competition authority to make some of the personal data concerning them available to a third party as a remedy to a competition law infringement.[193] On the other hand, the data recipient will have to inform the data subjects about the further processing it will conduct on the data covered by the remedy.[194]

Moreover, both the data holder and the data recipient will have to comply with the purpose limitation principle.[195] This outlines the importance of defining in advice, and ideally already in the competition authority's decision, for which specific purpose the data shall be shared (e.g. which products or services does the data recipient intend to offer thanks to the data). Additionally, the data holder and the data recipient will have to comply with the data minimisation principle.[196] In this regard, the data sharing remedy should only cover the data that is necessary to fulfil the specific purpose of the processing defined by the competition authority's decision. In the same vein, the accuracy of the shared data should be ensured and the data recipient should store it for no longer than is necessary for this specific purpose.[197]

Finally, the data holder and the data recipient will have to implement appropriate technical and organisational measures in order to ensure the security of the data during the sharing and during the further processing[198], and they will have to document how the concrete implementation of the data sharing remedy complies with all of the above-mentioned principles, in light of the accountability principle.[199]

In conclusion, while some tensions might emerge between the two regimes, they are not incompatible, and they can be reconciled by making a competition law duty to share data compliant with data protection

[191] Kathuria and Globocnik (2019:25).
[192] Articles 5.1.a) and 12 to 14 of the GDPR.
[193] Article 13 of the GDPR.
[194] Article 14 of the GDPR.
[195] Article 5.1.b) of the GDPR.
[196] Article 5.1.c) of the GDPR.
[197] Article 5.1.d) and e) of the GDPR
[198] Articles 5.1.f) and 32 of the GDPR.
[199] Article 5.2 of the GDPR

principles. This implies the need for competition and data protection authorities to collaborate on this matter.

5. Conclusion

This paper shows that data sharing presents many opportunities, in particular in reaping the benefits of big data analysis, stimulating innovation or ensuring an innovation level playing field between undertakings which have many data and those which have less. However, data sharing also presents several risks in facilitating explicit or tacit collusion between firms or the exploitation of consumers as well as in undermining of privacy. Moreover, compulsory data sharing may decrease the incentives of data holders to collect, store and analyse data as well as the incentives of data seekers to collect, store or analyse themselves instead of relying of the work done by others. Therefore, the optimal regulatory framework relating to data sharing should maximise those benefits of data sharing while minimising those risks.

Such regulatory framework is based on a combination of many legal instruments, some being horizontal (in particular competition protection, consumer protection and data protection laws) and others being sectoral (for instance in the financial, automotive, energy or agricultural sectors). It should be recognised that, if they are implemented effectively, the horizontal instruments could already facilitate or even impose the sharing of data in many circumstances. Those existing horizontal rules should be complemented with new sectoral rules only when they have proved to be insufficient given the particular characteristics of the sector.

In addition, it is of the utmost importance that those horizontal and sectoral legal instruments are applied consistently. This means, on the one hand, that any conflict should be alleviated or minimised and, on the other hand, that instruments should be applied more as complements than as substitutes. As those legal instruments, in particular the horizontal ones, are based on open norms which leave an important margin of interpretation by the regulatory authorities and the judges, it is recommended that those institutions interpret the law in a manner that minimises conflict and maximises complementarity.

Such an objective can only be achieved if the authorities in charge of the enforcement of the different legal instruments cooperate closely with each other to ensure consistent and complementary interpretation of the instruments they are in charge with. In case of conflict, dialogue between the authorities could minimise them and arbitrate them in a transparent manner.

References

Abrahamson Z. (2014), 'Essential Data', *Yale Law Journal* 124, 867-881.

Autorité de la concurrence and Bundeskartellamt (2016), *Competition Law and Data*.

Bourreau M. and A. de Streel (2019), *Digital Conglomerates and EU Competition Policy*, Mimeo.

Bresnahan T.F. and M. Trajtenberg (1995), 'General purpose technologies: Engines of growth?', *Jour. of Econometrics* 65(1), 83-108.

Crémer J., Y-A de Montjoye and H. Schweitzer (2019), *Competition policy for the digital era*, Report for the European Commission.

Colangelo G. and O. Borgogno, "Data, Innovation and Transatlantic Competition in Finance: The Case of the Access to Account Rule", *Stanford-Vienna European Union Law Working Paper No. 35*, 2018.

Costa-Cabral F. (2016), 'The Preliminary Opinion of the European Data Protection Supervisor and the Discretion of the European Commission in Enforcing Competition Law', *Maastricht Journal of European and Comparative Law.*

de Streel A. (2018), 'Big Data and market power' in B. Meyring, D. Gerard, E. Morgan de Rivery (eds), *Dynamic markets, Dynamic competition and dynamic enforcement*, Bruylant, 97-112.

Drexl J. (2016), *Designing Competitive Markets for Industrial Data - Between Propertisation and Access*, Max Planck Institute for Innovation and Competition Research Paper 16-13.

Drexl J. (2018), "Legal Challenges of the Changing Role of Personal and Non-Personal Data in the Data Economy", *Max Planck Institute for Innovation & Competition Research Paper 18-23*.

Graef I. (2016), *EU Competition Law, Data Protection and Online Platforms: Data as Essential Facility*, Kluwer Law International.

Graef I. (2018a), 'Blurring Boundaries of Consumer Welfare: How to Create Synergies between Competition, Consumer and Data Protection Law in Digital Markets', in: M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (eds.) *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?*, Springer, 121-151.

Graef I. (2018b), 'When data evolves into market power – data concentration and data abuse under competition law', in M. Moore & D. Tambini (Eds.), Digital Dominance: Implications and Risks, Oxford University Press.

Graef I., D. Clifford & P. Valcke (2018), 'Fairness and enforcement: bridging the boundaries between competition, data protection and consumer law', *International Data Privacy Law.*

Graef I., M. Husovec, and N. Purtova (2018), "Data Portability and Data Control: Lessons for an Emerging Concept in EU Law", *German Law Journal*, 19(6), 1359-139

Graef I., R. Gellert and M. Husovec (2019), "Towards a Holistic Regulatory Approach for the European Data Economy: Why the Illusive Notion of Non-Personal Data is Counterproductive to Data Innovation", *European Law Review,* 605-621.

Junqué de Fortuny E., D. Martens and F. Provost (2013), 'Predictive Modelling with Big Data: Is Bigger Really Better?' *Big Data* 1(4), 215-226.

Kathuria and J. Globocnik (2019), "Exclusionary Conduct in Data-Driven Markets: Limitations of Data Sharing Remedy", *Max Planck Institute for Innovation and Competition Research Paper No. 19-04*, 2019, available on SSRN.

Kerber W. and H. Schweitzer (2017), 'Interoperability in the Digital Economy', *JIPITEC*, 39

Ledger M. and T. Tombal (2018), "*Le droit à la portabilité dans les textes européens : droits distincts ou mécanisme multi-facettes ?*", *R.D.T.I*. 72, 25-44.

Lynskey O. (2017), "Aligning data protection rights with competition law remedies? The GDPR right to data portability", *European Law Review*, 793-814.

Lundqvist B. (2018), 'Competition and Data Pools', *Journal of European Consumer and Market Law*.

Mayer-Schonberger V. and T. Ramge (2018) *Re-inventing capitalism in the age of big data*, Ed. John Murray.

Metzger A., Z. Efroni, L. Mischau & J. Metzger (2018), "Data-Related Aspects of the Digital Content Directive", *JIPITEC*, 102-105.

Muralidhar K., R. Sarathy and H. Li (2014) "'To Share or Not to Share. That is Not the Question' - A Privacy Preserving Procedure for Sharing Linked Data", available on SSRN.

OECD (2015), *Data-Driven Innovation: Big Data for Growth and Well-Being*, Paris, OECD Publishing.

Prüfer J. and C. Schottmuller (2017), *Competing with Big Data*, CentER Discussion Paper 2017-007.

Rubinfeld D.L. and M.S. Gal (2017), "Access Barriers to Big Data", *Arizona Law Review* 59, 339-381.

Schweitzer H., Haucap J., Kerber W. and Welker R. (2018), *Modernising the law on abuse of market power*, Report for the German Federal Ministry for Economic Affairs and Energy.

Van der Auwermeulen B. (2017), "How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer Law & Security Review*, 57-72.

Varian H. (2019), 'Artificial Intelligence, Economics, and Industrial Organization', in A.K. Agrawal, J. Gans and A. Goldfarb (ed), *The Economics of Artificial Intelligence*, University of Chicago Press.

Vezzoso S., "Fintech, Access to Data, and the Role of Competition Policy", 2018, available on SSRN.

Wendehorst C. (2017), "Of Elephants in the Room and Paper Tigers: How to Reconcile Data Protection and the Data Economy', in *Trading Data in the Digital Economy: Legal Concepts and Tools*, S. Lohsse, R. Schulze and D. Staudenmayer (eds.), Baden-Baden, Nomos.

Zech H. (2016), 'Data as tradeable commodity' in A. De Franceschi (ed), *European Contract Law and the Digital Single Market*, Intersentia, 49-80.

Zingales N. (2017), ‘Between a rock and two hard places: WhatsApp at the crossroad of competition, data protection and consumer law’, *Computer Law & Security Review*, 557-558